

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

**(19) World Intellectual Property Organization
International Bureau**



(43) International Publication Date
7 December 2000 (07.12.2000)

PCT

(10) International Publication Number
WO 00/74345 A1

(51) International Patent Classification⁷: H04L 29/06

(21) International Application Number: PCT/SE00/01093

(22) International Filing Date: 26 May 2000 (26.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

| | | |
|------------|--------------------------|----|
| 60/136,444 | 28 May 1999 (28.05.1999) | US |
| 09/569,768 | 12 May 2000 (12.05.2000) | US |

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors: SANCHEZ HERRERO, Juan Antonio; Calle Desengano, 24 1 Centro, E-28004 Madrid (ES). CALATRAVA REQUENA, Odelin; Calle General Kirkpatrick, 6, E-28027 Madrid (ES).

(74) Agent: NORIN, Klas; Ericsson Radio Systems AB, Common Patent Department, S-164 80 Stockholm (SE).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

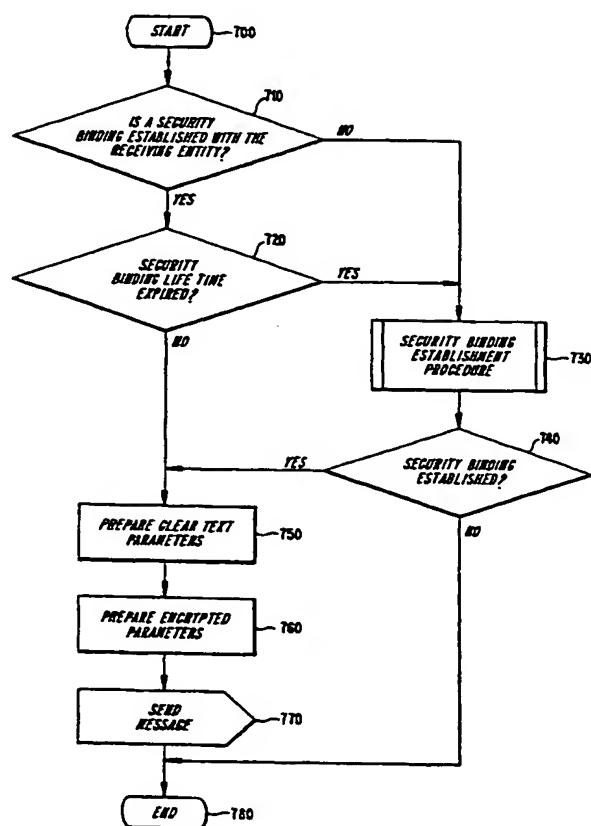
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
 — *With international search report*

Published:
— *With international search report.*

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR SECURE COMMUNICATION



(57) Abstract: Secure communication is provided for entities in one or more networks. It is determined whether security measures needed for the communication exist between the entities. If such measures do not exist, the security measures are established, and the communication is initiated. The security measures include security bindings including information needed for the secure communication. Security measures are established between entities in one or more networks based on predetermined security requirements and on a determined needed security level. The security level needed may be determined based on whether the entities are in the same network or in different networks and/or on the information being transmitted. Security bindings are established between the entities depending on the information to be transmitted and/or the network to which the entities belong. The security bindings include information identifying the security binding, encryption information, authentication information, integrity information, a list of addressees or group of addressees included in the security bindings, and/or information regarding the lifetime of the security bindings. The encryption, authentication, and integrity may be specified at a parameter level.

(19)日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11)特許出願公表番号
特表2003-501891
(P2003-501891A)

(43)公表日 平成15年1月14日 (2003.1.14)

(51)Int.Cl.
H 04 Q 7/38
H 04 L 9/14

識別記号

F I
H 04 B 7/26
H 04 L 9/00
1 0 9 R 5 J 1 0 4
1 0 9 S 5 K 0 6 7
6 4 1

テ-マコト (参考)

(21)出願番号 特願2001-500524(P2001-500524)
(86) (22)出願日 平成12年5月26日(2000.5.26)
(85)翻訳文提出日 平成13年11月21日(2001.11.21)
(86)国際出願番号 PCT/SE00/01093
(87)国際公開番号 WO00/074345
(87)国際公開日 平成12年12月7日(2000.12.7)
(31)優先権主張番号 60/136,444
(32)優先日 平成11年5月28日(1999.5.28)
(33)優先権主張国 米国(US)
(31)優先権主張番号 09/569,768
(32)優先日 平成12年5月12日(2000.5.12)
(33)優先権主張国 米国(US)

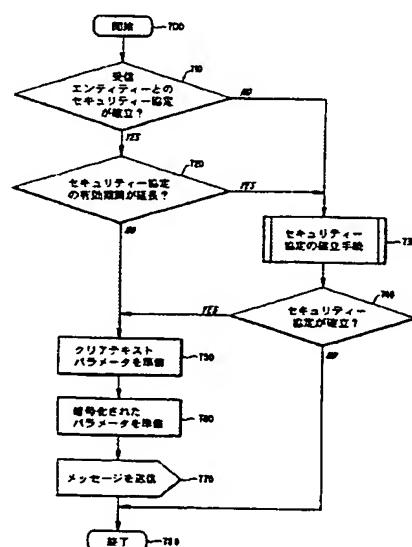
(71)出願人 テレフォンアクトーボラゲット エル エ
ム エリクソン (パブル)
スウェーデン国エス - 126 25 スト
ックホルム
(72)発明者 サンチエス, エレロ, フアン アント
ニオ
スペイン国 マドリッド エ-28004,
24 1 セントロ, カージェ デセンガ
ノ
(74)代理人 弁理士 大塚 康徳 (外3名)

最終頁に続く

(54)【発明の名称】 安全に通信するための方法及び装置

(57)【要約】

安全な通信が1以上のネットワークのエンティティに提供される。通信に必要とされるセキュリティの尺度がエンティティ間に存在するかどうかが決定される。もしそのような尺度が存在しないならば、セキュリティの尺度が確立され、通信が開始される。セキュリティの尺度は、セキュリティ協定を含み、セキュリティ協定は、安全な通信を実現するために必要な情報を有する。セキュリティの尺度は、前もって決定されたセキュリティ要件および決定された必要なセキュリティレベルに基づいて、1以上のネットワーク内のエンティティ間で確立される。必要なセキュリティレベルは、エンティティが同一のネットワークまたは異なるネットワークに存在するか、および/または、送信される情報であるかどうかに基づいて、決定されてもよい。セキュリティ協定は、送信される情報および/またはエンティティが所属しているネットワークに依存して、エンティティ間に確立される。セキュリティ協定は、セキュリティ協定を識別するための情報、暗号化情報、認証情報、完全性情報、セキュリティ協定に含まれるアド



【特許請求の範囲】**【請求項1】**

1以上の通信ネットワークにおいてエンティティ間の安全な通信を提供するための装置であって、

前記エンティティ間で通信するために必要なセキュリティーの尺度が存在するかどうかを決定するための手段と、

前記尺度が存在しない場合に、セキュリティーの尺度を確立するための手段と、

前記セキュリティーの尺度が確立されると、前記エンティティ間の通信を確立するための手段と、

を含むことを特徴とする装置。

【請求項2】

前記セキュリティーの尺度は、安全な通信のために必要な情報を有するセキュリティー協定を含むことを特徴とする請求項1に記載の装置。

【請求項3】

前記決定するための手段は、前記通信のために必要なセキュリティーレベルを決定するための手段を含み、

前記確立するための手段は、前記セキュリティーレベルを要求するための手段と、前記セキュリティーレベルの要求に応じて、前もって決定されたセキュリティー要件に基づいて前記セキュリティーの尺度を確立するための手段と、

を含むことを特徴とする請求項1に記載の装置。

【請求項4】

前記セキュリティーの尺度を確立するための手段は、前もって決定されたセキュリティー要件に基づいて、1以上のネットワークにおけるエンティティ間にセキュリティーの尺度を確立することを特徴とする請求項1に記載の装置。

【請求項5】

前記セキュリティーの尺度を確立するための手段は、送信される情報および/またはエンティティが属しているネットワークに依存して、少なくとも通信中のエンティティ間でセキュリティー協定を確立することによって、前記エンティテ

イ間に前記要求されたセキュリティーを確立することを特徴とする請求項1に記載の装置。

【請求項6】

前記セキュリティー協定は、前記セキュリティー協定を識別するための情報を含むことを特徴とする請求項2に記載の装置。

【請求項7】

前記セキュリティーの尺度は、暗号を含むことを特徴とする請求項1に記載の装置。

【請求項8】

前記セキュリティー協定は、暗号化情報を含むことを特徴とする請求項2に記載の装置。

【請求項9】

前記暗号は、パラメータレベルで指定されることを特徴とする請求項7に記載の装置。

【請求項10】

前記セキュリティーの尺度は、認証を含むことを特徴とする請求項1に記載の装置。

【請求項11】

前記セキュリティー協定は、認証情報を含むことを特徴とする請求項2に記載の装置。

【請求項12】

前記認証は、パラメータレベルで指定されることを特徴とする請求項10に記載の装置。

【請求項13】

前記セキュリティーの尺度は、完全性を含むことを特徴とする請求項1に記載の装置。

【請求項14】

前記セキュリティー協定は、完全性情報を含むことを特徴とする請求項2に記載の装置。

【請求項15】

前記完全性は、パラメータレベルで指定されることを特徴とする請求項13に記載の装置。

【請求項16】

前記セキュリティー協定は、前記セキュリティー協定に含まれているアドレスのグループ又はリストを含むことを特徴とする請求項2に記載の装置。

【請求項17】

前記決定するための手段は、セキュリティーの尺度の有効期間が満了したかどうかを決定することを特徴とする請求項1に記載の装置。

【請求項18】

前記セキュリティー協定は、前記セキュリティー協定の有効期間に関する情報を含むことを特徴とする請求項2に記載の装置。

【請求項19】

前記決定手段は、前記通信が同一ネットワークにおけるエンティティ間のものであるか、または異なるネットワークにおけるエンティティ間のものであるかを決定し、前記決定に基づいてセキュリティーレベルを要求することを特徴とする請求項3に記載の装置。

【請求項20】

1以上のネットワークにおけるエンティティ間で安全な通信を提供する方法であって、

前記エンティティ間において、前記通信のために必要なセキュリティーの尺度が存在するかを決定するためのステップと、

前記尺度が存在しない場合、前記セキュリティーの尺度を確立するためのステップと、

前記セキュリティーの尺度が確立すると前記通信を確立するためのステップと
、
を含むことを特徴とする方法。

【請求項21】

前記セキュリティーの尺度を確立するためのステップは、前記エンティティ間

にセキュリティ協定を確立することを特徴とする請求項20に記載の方法。

【請求項22】

前記決定するためのステップは、通信のために必要なセキュリティレベルを決定するためのステップを含み、前記確立するためのステップは、前記セキュリティレベルを要求するためのステップと、前記要求されたセキュリティレベルに応じ、前もって決定されたセキュリティ要件に基づいて前記セキュリティの尺度を確立するためのステップと、

を含むことを特徴とする請求項20に記載の方法。

【請求項23】

前記セキュリティの尺度を確立するステップは、前もって決定されたセキュリティ要件に基づいて、1以上のネットワークにおけるエンティティ間にセキュリティの尺度を確立することを特徴とする請求項20に記載の方法。

【請求項24】

前記セキュリティの尺度を確立するためのステップは、送信される情報および／またはエンティティが属しているネットワークに依存して、少なくとも通信中のエンティティ間でセキュリティ協定を確立することによって、前記エンティティ間に前記要求されたセキュリティの尺度を確立することを特徴とする請求項20に記載の方法。

【請求項25】

前記セキュリティ協定は、前記セキュリティ協定を識別するための情報を含むことを特徴とする請求項21に記載の方法。

【請求項26】

前記セキュリティの尺度は、暗号化を含むことを特徴とする請求項20に記載の方法。

【請求項27】

前記セキュリティ協定は、暗号化情報を含むことを特徴とする請求項21に記載の方法。

【請求項28】

前記暗号化は、パラメータレベルで指定されることを特徴とする請求項26に

記載の方法。

【請求項29】

前記セキュリティーの尺度は、認証を含むことを特徴とする請求項20に記載の方法。

【請求項30】

前記セキュリティー協定は、認証情報を含むことを特徴とする請求項21に記載の方法。

【請求項31】

前記認証は、パラメータレベルで指定されることを特徴とする請求項29に記載の方法。

【請求項32】

前記セキュリティーの尺度は、完全性を含むことを特徴とする請求項20に記載の方法。

【請求項33】

前記セキュリティー協定は、完全性情報を含むことを特徴とする請求項21に記載の方法。

【請求項34】

前記完全性は、パラメータレベルで指定されることを特徴とする請求項32に記載の方法。

【請求項35】

前記セキュリティー協定は、前記セキュリティー協定に含まれているアドレスのグループ又はアドレスのリストを含むことを特徴とする請求項21に記載の方法。

【請求項36】

前記決定するためのステップは、セキュリティーの尺度の有効期間が満了したかどうかを決定することを特徴とする請求項20に記載の方法。

【請求項37】

前記セキュリティー協定は、前記セキュリティー協定の有効期間に関する情報を含むことを特徴とする請求項21に記載の方法。

【請求項38】

前記決定するためのステップは、前記通信が同一ネットワークのエンティティ間のものであるか、または異なるネットワークのエンティティ間のものであるかを決定し、前記決定に基づいてセキュリティーレベルを要求することを特徴とする請求項22に記載の方法。

【発明の詳細な説明】

【0001】

背景

本発明は、一般に安全に通信するための方法及び装置と関連している。より明確には、本発明は、同一又は異なる通信ネットワークのエンティティ間で安全に通信するための方法及び装置と関連する。

【0002】

例えば、汎欧州移動体通信システム（GSM）、移動体通信のためのデジタルセルラー（DCS 1800）、パーソナル・コミュニケーションシステム（PCS）、および一般移動体通信システム（UMTS）など、多数の公衆陸上移動体ネットワークが存在する。これらのネットワークは、移動無線通信ネットワークの各セル間を移動している移動体加入者に様々なサービスと機能を提供する。移動無線通信システムのための例示的なネットワークアーキテクチャが図1に示されている。

【0003】

典型的なネットワークには、加入者についての情報をネットワークに格納するための少なくとも1つのホーム・ロケーション・レジスタ（HLR）100と、他のネットワーク内を移動しているであろう加入者についての情報を他のネットワークに格納するための在囲ロケーション・レジスタ（VLR）110と、移動局のために交換機能を実行する移動通信交換局（MSC）120と、PLMNからMSCへの着信呼を経路制御するためのゲートウェイMSC（GMSC）130と、交換局（SC）150を経由して移動局へのショートメッセージを配達するためのショートメッセージサービス局へのアクセスを提供するためのネットワークと移動体ネットワークとの間のインターフェースとなるSMSゲートウェイMSC（SMSGMSC）140とを含んでいる。基地局コントローラ（BSC）160と無線基地局装置（BTS）170は、ネットワークを移動局180に接続させるための基地局システム機器の一部である。装置IDレジスタ（EIR）190は移動局の装置IDの管理を担当する。

【0004】

図1に例示するように他のエンティティがネットワークに接続していてもよい。例えば、交換ネットワーク210はGMSC 130を経てネットワークに接続してもよく、パケットネットワーク220は、一般パケット無線サービスサポートノード(GSN)200を経てネットワークに接続してもよく、別のPLMN 230が別のGMSC 130と接続することも可能である。不正検出システム(FDS)240は、例えば、HLR 100、および別のMSC 120など、いくつかのタイプのネットワークエンティティに接続し、特定の加入者についての情報をエンティティから取得してもよい。収集される情報には、例えばMSCなどで作成された課金データレコードに関する情報や、例えば一般にHLRで作成される加入者の位置情報、リアルタイムで作成される動作に関する情報(所定期間内において実行された呼の転送登録数や、その時間内における並行呼の数その他など)が含まれてもよい。FDS 240はariうる不正リスクの状況を発見する。例えば、突然、加入者が、以前に決して起こらなかったような実に高い課金レコードを有しているときにFDS 240はそれを検出する。別の例として、加入者が一定の国にいくつかの並行した呼を生成するときに、FDS 240はそれを検出するが、これは呼の売却動作を示しているかもしれない。第3の例として、非常に短い時間内に、加入者が遠く離れた異なる2箇所に位置しているときにも、FDS 240はそのことを検出するが、これはクローン動作を示しているかもしれない。

【0005】

PLMNの複数のエンティティは共通のシグナリング(信号伝達)システムを経由して通信する。例えば、GSMシステムにおいては、CCITTにより規定されたシグナリングシステムNo. 7の移動体応用部(MAP)は、PLMNの複数のエンティティ間で通信するために使用される。このシグナリングシステムの詳細は、デジタルセルラー電話通信システム(フェーズ2+)、移動体応用部(MAP)仕様、TS GSM 09.02 v. 5.6.00において記載されており、ここに参照により取り込む。

【0006】

移動体ネットワークのオペレータ間ローミング協定に基づき、ホームPLMN

(HPLMN) と称される特定のPLMN 250に属している移動体加入者が、ビジターPLMN (VPLMN) と称される他のPLMNネットワーク260をローミングしている間は、PLMNネットワーク260のサービスと機能を利用できる。図2はローミング・シナリオについてのネットワークアーキテクチャの例示的なコンフィギュレーションを示している。図1と同様に、FDS 240はHLR 100やMSC 120などのエンティティと接続している。

【0007】

ネットワーク要素、送信メディアその他の継続的な成長によって、より多くの改良がなされた不正な方法が開発されてきた。そのような方法はシグナリングシステムの攻撃に関与している。例としてGSMを用いると、敏感なシグナリングメッセージを伝送するシステムとしてのグローバルSS7ネットワークのセキュリティーが、主に危険にさらされている。制御を伴わない媒体では、メッセージの盗聴、変更、挿入または削除が可能である。GSM標準においては、最近、機密情報がシグナリングプロトコルに追加されたが、信号伝達媒体の機密性が不足しているため、機密リスクを増大させてしまうだろう。そのような機密情報には、例えば、地理的な座標に基づく位置情報や課金情報などが含まれている。例えば、送信制御プロトコル／インターネットプロトコル(TCP/IP)など、信号伝達のためのオープンな信号伝達プロトコルを将来使用することによって、これらのリスクはさらに増大するだろう。現在のGSM仕様では、移動体加入者識別情報の認証を提供しているが、ネットワークエンティティの認証についてはGSMにおいて定義まったく定義されてはいない。いくつかの制限方針が存在してはいるものの、ID情報が改ざんされなかったことを保証するためのメカニズムはまったく存在していないのである。

【0008】

シグナリングネットワークへのアクセスによって実行された攻撃から保護される移動体通信ネットワークを通して、一定の機密情報を送信する方法のニーズがある。ユーザー機密は、シグナリングメッセージに含まれている一定の情報にアクセスすることによって攻撃可能である。この情報は主に呼の生起／宛先および加入者の位置と関連する。ネットワークオペレーションへの他の攻撃としては、

ネットワークノードまたはネットワークエンティティのなりすましであろう。加入者のなりすましによって直面する主要な脅威は、認証手続の返答の操作と、認証情報の盗聴である。そのようななりすましは機密情報へのアクセスを許し、具体的なサービス行為（例えば、移動体ネットワーク強化ロジック（CAMEL）にカスタマイズされたアプリケーションである課金サービス、位置サービス、補足サービス（SS）手続、冗長性、その他）に対する課金が生じ、その結果として不正が生じ、および／または、ネットワーク動作に影響を及ぼすかもしれない。

【0009】

サービスの可用性は、サービスを与える加入情報情報またはメッセージの操作に基づいて、ユーザーレベルで危うくされる。また、サービスの可用性は、例えば、加入者の位置を示すメッセージの削除、またはメッセージの挿入を通してネットワークに過負荷をかけるなど、リソースの解放関連メッセージを削除することによって、ネットワークレベルで危険にさらされる。

【0010】

従って、1以上のネットワークエンティティ間の秘密通信を開始するために、発信ノードまたはネットワークエンティティを認証するニーズがある。

【0011】

要約

従って、本願発明の目的は、安全な通信を提供することである。さらに、本願発明の別の目的は、機密通信のためにネットワークエンティティを認証するための技術を提供することである。

【0012】

本願発明の例示的な実施形態によれば、これらおよび他の目的は、1以上のネットワークのエンティティ間で安全に通信するための方法及び装置により達成される。エンティティ間の通信に必要とされるセキュリティの尺度が存在するかどうかが決定される。もしそのような尺度が存在しないならば、セキュリティの尺度が確立され、通信が開始される。セキュリティの尺度には、安全な通信のために必要な情報を含んだセキュリティーバインディング（協定）が含まれる

。前もって決定されたセキュリティ要件および決定された必要なセキュリティレベルに基づいて、1以上のネットワークのエンティティ間でセキュリティの尺度が確立される。必要なセキュリティレベルは、エンティティが同一のネットワーク又は異なるネットワークあるか、および／または、送信される情報であるかどうかに基づいて決定されてもよい。セキュリティ協定は、送信される情報および／またはエンティティが属しているネットワークに依存し、エンティティ間で確立される。セキュリティ協定は、セキュリティ協定を識別するための情報、暗号化情報、認証情報、完全性情報、セキュリティ協定に含まれるアドレスのリスト又はアドレスのグループおよび／またはセキュリティ協定の有効期間に関する情報などを含んでもよい。暗号化、認証、および完全性はパラメータレベルで指定されてもよい。

【0013】

詳細な説明

セキュリティ分析の一般的な前提是、セキュリティーチェーンの中の最も弱い個所が完全なセキュリティーシステムを危険にさらすかもしれないことであろう。シグナリングシステムにおいて、チェーンは、統合デジタル通信網（ISDN）ユーザー部（ISUP）、データ転送応用部（DTAP）、基地局システム応用部（BSSAP）、GPRS転送プロトコル（GTP）、CAMEL応用部（CAP）、インテリジェント・ネットワーク・アプリケーション・プロトコル（INAP）など、多数のシグナリングプロトコルを含む。説明に役立てる目的で、以下の説明は、翻訳機能応用部（TCAP）と移動体応用部（MAP）プロトコルに向けられる。しかし、本発明は、これらのプロトコルを使用するアプリケーションに限定されなるものではなく、他のプロトコルを適用してもよい。

【0014】

例示的な実施形態によると、セキュリティーは、データ暗号化、認証、完全性、およびキー管理の4つのメカニズムの1以上を使用して管理がなされる。送信された情報の機密性を保証するためにデータの暗号化が用いられ、一定のエンティティから受信されたメッセージが不正な者によって挿入されたり置換されたりしていないことを保証するために認証が用いられ、情報が改ざんされていないこ

とを保証するために完全性が利用され、暗号化、認証、および完全性メカニズムを管理するためにキー管理が用いられる。キー管理メカニズムは、暗号化と認証メカニズムが基づいて、キーの柔軟な取り扱いが可能となる。

【0015】

どのようにこれらのメカニズムを適用するかについては、考慮に値するものが多くある。例えば、シグナリング・セキュリティー・メカニズムをサポートしていないエンティティと通信する際には、後方互換性が維持されるべきである。また、さらなる適応へのニーズと、テクノロジーの出現（例えば、新しい暗号化アルゴリズム、将来のセンシティブな情報送信など）に対処すべく、前方互換性も可能にされるべきである。セキュリティーメカニズムがもたらすネットワーク性能への影響は最小にされるべきである。高いセキュリティー要件を有するネットワークエンティティの数も最小にされるべきである。ローミング・シナリオの取り扱いは簡潔化されるべきである。ネットワーク、エンティティ、プロシージャおよび加入者レベルでのアプリケーションのセキュリティーメカニズムにおいて、高い細分性が提供されるべきであり、様々なセキュリティーレベルが共存してもよい。

【0016】

例示的な実施形態によると、すべてのメカニズムが適用されなければならないわけではない。例えば、もしメッセージに含まれている情報自体が重要であると考えられるならば、これは、他の要件とは無関係に、場合によってはデータ暗号化（盗聴の回避）だけが適用されること、あるいはデータの完全性（操作の回避）だけが適用されることが望ましいかもしれないことを暗示している。例示的な実施形態によると、メカニズムのアプリケーションの独立を可能とし、及び、新興のテクノロジーへの適用を簡素化するために、メカニズムはできる限り独立したものとする。

【0017】

例示的な実施形態によると、キー管理システムが提案されており、完全性の手続を簡素化するためには、暗号化と認証メカニズムが有利である。一般に、キー管理は他のメカニズムによって共通に使用されるので、最初にキー管理メカニズ

ムを説明する。

【0018】

キー管理

キー管理とは、生成、登録、証明、登録解除、配布、インストール、記憶、アーカイブ、撤回、派生、およびキー素材の破壊などのサービスを使用すること及びこれらを管理することである。キー管理の目的はこれらのキー管理サービスを安全に管理し使用することである。

【0019】

キーの保護は極めて重要である。キーの適切な保護はキーが直面する脅威に依存する。キーの配布において生じる問題は、通信に関するエンティティの数とそれらの性質にある。GSM／UMTSネットワークなどの移動体ネットワークは、ローミングを許可しているので、オペレータのセキュリティードメイン外にあるエンティティ間で通信が実行されることがある。一方で、各オペレータは、エンティティにおいてセキュリティーを完全に制御する必要があるかもしれない。

【0020】

エンティティの間のセキュリティー協定は、エンティティ間における許可された通信、使用されている暗号化、認証、および完全性メカニズムの特性、協定に対応する特有な特性を示す。例示的な実施形態によれば、セキュリティー協定には、セキュリティー協定を唯一無二に識別する協定IDに関する情報、暗号化されるパラメータを特定する暗号に関する情報、応用可能なアルゴリズム（例えばBEANOなど）に関する情報、使用されるセッションキーに関する情報、認証を必要とするメッセージを参照する認証に関する情報、応用可能な認証システムに関する情報、使用されているキーに関する情報、完全性を必要とするメッセージを参照する完全性に関する情報、応用可能な完全性システムに関する情報、セキュリティー協定を応用することが可能な時間である有効期間に関する情報、及び、セキュリティー協定に含まれるアドレス及びアドレスグループについてのリストが含まれる宛先に関する情報などが含まれる。

【0021】

エンティティ間で共通のシグナリングシステムを使用することにより、所定のキーを用いた莫大な量のメッセージが生起され、これにより大量な情報による攻撃を許すことになる。これは、通常、大きなキーとブロックサイズに基づいた非常に強力な認証メカニズムを使用することで避けられるが、システム・パフォーマンスに不適当な影響を与えててしまうことを暗示している。

【0022】

大量の情報に基づく攻撃の問題は、頻繁なキーの変更により回避可能である。従って、例示的な実施形態においては、特定の通信セッションの間でだけ有効であり続けるようなセッションキーが使用されてもよい。

【0023】

セッションキーは、規定された期間の間だけ有効にされる。従って、キーは一時的なものであり、規定された期間が経過した後には変更が必要となる。従って、ライフサイクルは各キーごとに関係付けられる。キーの典型的なライフサイクルは図3において例示されている。

【0024】

ライフサイクルは3つの主要な状態として、ペンディングアクティブ（起動待機）、アクティブ（起動）、ポストアクティブ（起動後）がある。キーが生成されると、アクティブ待機状態300に移行する。アクティブ待機状態300において、キーは生成されているが、使用するためにはアクティブにされていない。キーは、破壊されるか、または暗号化オペレーションのために起動するまで、アクティブ待機状態にとどまる。活性化（起動）されると、キーはアクティブ状態310に移行する。アクティブ状態310において、キーは、情報を暗号処理するために使用される。キーは、例えば、キーが満了したりまたは撤回されたりしたことを理由に、キーの使用を制限するために非活性化（起動終了）されるまでは、アクティブ状態にとどまる。非活性化において、キーは使用を制限され、ポストアクティブ状態320に移行する。ポストアクティブ状態320において、キーは復号または確認のために使用されるだけである。キーは、それが破壊されるか、または再活性化されるまで、ポストアクティブな状態にとどまる。再活性化は、暗号化オペレーションのために再びポストアクティブなキーを使用可能と

するものであり、これによりアクティブ状態310に戻される。

【0025】

エンティティの数は、協力エンティティ間のセキュリティ協定の必要性を指数的に増大させる。もし個々の通信ペアについて、エンティティ間のセキュリティ協定が独立であるならば、これは処理と性能に対し悪い影響を与えるであろう。しかし、複数のセキュリティ協定において同一のキーを使用すれば、キーが破壊される可能性が増大することになり、セキュリティシステム全体の故障を結果として生じるかもしれない。

【0026】

この問題に目を向ければ、オペレータのセキュリティドメイン外の団体により認証されるべきであるエンティティ数は最小化されるべきである。それゆえ、例示的な実施形態においては、各ネットワークのほんのわずかのエンティティがけが、信頼できる第三者機関（ＴＴＰ）のシステムにより認証される。

【0027】

例示的な実施形態によると、オペレータドメインで扱えるキーの機能は、既存の認証センター（AuC）に基づくものであってもよい。例えば、移動端末の加入者が電源を投入し、移動体がネットワークに参加したときなど、移動端末のネットワークへの参加フェーズにおいて、AuCは、加入者を認証するための情報を含んでいる。すでにAuCは、本願において使用可能なほどの強力なセキュリティ要件を備えているので、これは有利である。さらにGSMシステムにおいて、AuCの取り扱いMAPプロトコルは、キー配布を処理するためにVLR、MSC、HLRなどのエンティティと通信するための使用可能である。

【0028】

ネットワークエンティティ間のセキュリティ協定についての例示的な基本キー管理アーキテクチャは、図4に示されている。外部PLMNレベル、内部PLMNレベル、およびセッションレベルの3種のセキュリティーレベルがある。

【0029】

外部PLMNレベルは、異なる複数のPLMNに属しているエンティティ間でセキュリティ協定を確立するために使用される。例えば、図4に例示するよう

に、TTPとネットワークAのAuCAとの間、およびTTPとネットワークBのAuCBとの間に、これらのセキュリティ協定確立される。これらのセキュリティ協定は、前もって決定されたセキュリティ要件、例えば、PLMNオペレータ間の相互協定やTTPとして作動しているエンティティや外部の協力を信頼することによるなど、他のエンティティを認証するために使用されるいずれかのエンティティに基づいて確立される。これらのセキュリティ協定は強力なセキュリティ要件を備えており、使用される具体的なメカニズムは、最先端技術の使用を許すために十分に柔軟であるべきである。TTPはネットワーク外で他のシステムと統合されてもよい。それにもかかわらず、マルチベンダ環境においてこのセキュリティ協定を提供するためには、デフォルトメカニズムがサポートされるべきである。

【0030】

例示的な実施形態によると、内部PLMNレベルは、同じPLMNに属しているエンティティ間のセキュリティ協定を確立するために使用される。内部PLMNレベルでは、1以上のAuCエンティティ（確立されたセキュリティ協定を伴う）が、PLMNのエンティティについてTTPとして作動する。例えば、図4に示されるように、AuCAとAuCB間にはセキュリティ協定が存在する。これらのセキュリティ協定は、異なる標準の制定やカスタマイズされたセキュリティ方式も可能とするためにオペレータ内部で確立されてもよい。それにもかかわらず、マルチベンダ環境においてセキュリティ協定を提供するために、いくつかの標準のメカニズムがサポートされるべきである。

【0031】

セッションレベルは、通信しているエンティティ間のセキュリティ協定を確立するために使用される。確立されたセッションは、エンティティに割り当てられたAuC（または複数のAuC）を通して処理される。個々のエンティティは、その対応したAuCを信頼する。例えば、図4に示されるように、ネットワークAのネットワークエンティティNEAは、セキュリティ協定を経てAuCAと接続する。同様に、ネットワークBのネットワークエンティティNEBは、セキュリティ協定によってAuCBと接続している。また、ネットワークエン

ティティ $N \in A$ と $N \in B$ は、セキュリティ協定を介して相互に接続される。図4において、説明を簡潔にするために個々のネットワークに1つの $A \cup C$ が示されているが、1以上の $A \cup C$ が各ネットワークに採用されても良いし、ネットワークの各エンティティに1以上の $A \cup C$ が割り当てられてもよい。

【0032】

セッションレベルには、2タイプの可能な通信があり、通信のタイプに依存している（外部PLMNまたは内部PLMN）。もし外部PLMNで通信されるならば、すなわち、異なるネットワークにおけるエンティティ間で通信されるならば、選択された識別メカニズムは、異なる標準のセキュリティ方式を確立可能とすべきである。もし内部PLMNで通信されるならば、すなわち、同一ネットワーク内におけるエンティティ間での通信であれば、選択されたメカニズムは、異なる標準と、カスタマイズされたセキュリティ方式の確立を可能とすべきである。それにもかかわらず、マルチベンダ環境においてセキュリティ協定を提供するためには、複数の標準メカニズムがサポートされるべきである。

【0033】

それゆえ、選択されたメカニズムは、異なる標準と、カスタマイズされたセキュリティ方式の確立を可能とすべきである。例示的な実施形態によると、セキュリティ協定はMAPプロトコルに基づいていてよい。

【0034】

インストールの結果として、個々のエンティティは、その信号セキュリティについて責任がある $A \cup C$ に kontaktするために十分な情報を備える。異なるレベルについてのセキュリティ協定は、第1に内部HPLMNレベルが、次に、セッションレベルが確立される。

【0035】

図5Aに示されたシーケンスは、キー処理情報を送信するための例示的なメッセージフローを示している。第一に、送信側エンティティが受信側エンティティとともに、セキュリティ協定をすでに確立しているかどうかを検査するか、または、セキュリティ協定が満了したかを検査する。次に、送信エンティティは、セキュリティ協定要求メッセージを送信エンティティ $A \cup C$ に送信する。送

信エンティティ A u C は、送信エンティティへの希望されるセキュリティ協定についての情報を維持し、この情報は、各属性ごとに、属性が要求されるか又は交渉可能であるかを示している。送信エンティティ A u C は、セキュリティ協定要求メッセージを受信エンティティ A u C に送信する。受信エンティティ A u C はメッセージを受信エンティティに送信し、受信エンティティは、どの属性を処理できるかを決定し、受け容れられたセキュリティ協定属性でもって受信エンティティ A u C に応答する。そして、受信エンティティ A u C は、受け容れられた属性によって送信エンティティ A u C に応答する。送信エンティティの A u C が、受信エンティティにより指定された属性の受け容れを示すセキュリティ協定受け容れメッセージを送信エンティティに送信する。もし受け容れられた属性が通信に十分であると考えられるならば、送信エンティティはセキュリティ協定受け容れ承認メッセージによって送信エンティティ A u C に応答し、このメッセージが受信エンティティ A u C を経て受信エンティティに転送される。

【0036】

選択肢として、受信エンティティ A u C は、どの属性が容認できるかを決定でき、さらに、容認できる属性を示しているセキュリティ協定通知メッセージを、送信エンティティ A u C と受信エンティティに送信できる。例えば、受信エンティティがどの属性を処理できるかを特定している情報を、受信エンティティ A u C が持っているときに、この選択肢は適用可能であろう。

【0037】

例示的な実施形態によると、キー処理メッセージは、それに含まれる完全性情報とともに送信され、暗号化され、認証される。

【0038】

図5Bは、セキュリティ協定についての確立処理の詳細な例を示している。この図において、HLRとVLRの間にセキュリティ協定を確立する方法が例として示されている。この方法は、VLRにセキュリティ協定を確立するための要求をHLRが開始することから始まる。この要求は、提案されたアルゴリズムとして、例えば、Alg 1とAlg 2、およびセキュリティレベルについてのパラメータとして、例えば、認証情報と課金データのためのクラス2、位置

についてのクラス1、および残りのデータについてのクラス0などを含んでいる。HLRアドレスもまた含まれる。セキュリティ協定はまだ確立されていないので、セキュリティ協定識別情報はまったく存在しない。この要求は、HLRについてのAuCであるAuC₁によって受信され、VLRのためのAuCであるAuC₂へと送信される。AuC₂は、キー要求を含み、セキュリティ協定識別情報を割り当てるための要求をVLRに送信する。VLRは、どの提案されたアルゴリズム及びどのセキュリティクラスに対応できるのかを決定し、適切なメッセージとして、例えば、Alg_2の受け容れおよびセキュリティクラスの受け容れを示す受け容れメッセージを応答として送信する。受け容れメッセージによって、VLRアドレスも提供される。受け容れメッセージは、AuC₂からAuC₁へと転送され、AuC₁はHLRに受け容れメッセージを送信する。HLRは、AuC₁へと送信される受け容れ承認を用いて応答する。AuC₁はAuC₂へとこのメッセージを転送し、AuC₂は、このメッセージをVLRに送信する。受け容れ承認がVLRによって受信された後に、セキュリティ協定の確立が完成される。

【0039】

データ暗号化

複数のネットワークエンティティ間で送信される可能性のある機密情報には多数のタイプが存在し、例えば、位置情報、課金情報及びトリプレット、すなわち、加入者を認証するために使用された情報要素であって、乱数、数値化された応答、および暗号化キーをなどがある。例えば、この情報は、以下のメッセージにおいて、MAP及び機能応用部(CAP)プロトコルで識別される：

【0040】

【表1】

位置情報

| パラメータ | メッセージ | プロトコル |
|---|---|-----------------------------|
| RESULT Parameter:LocationInformation パラメータ : 位置情報 | ProvideSubscriberInfo 加入者情報の提供 (HLR->MSC/VLR) | MAP V1, V2, REL96, REL97 |
| RESULT Parameter:LocationInformation パラメータ : 位置情報 | SendRoutingInfo 経路情報の送信 (HLR->GMSC) | MAP REL96, REL97 |
| RESULT Parameter:LocationInformation パラメータ : 位置情報 | Anytime interrogation 常時質問 (gsmSCF->HLR) | MAP REL96 |
| ARGUMENT Parameter:LocationNumber パラメータ : 位置番号 | Initial DP DPの開始 (gsmSSF->gsmSCF) | CAP |

テーブル I

【0041】

【表2】

課金情報

| パラメータ | メッセージ | プロトコル |
|--|--|--------------|
| Result parameter 結果パラメータ PartyToChange 変更されるパーティ | FurnishChargingInfo 課金情報の提供 (SRR->SSP) | CAP REL97 |
| RESULT Parameter FreeFormatData パラメータ : 自由様式データ | FurnishChargingInfo 課金情報の提供 (SCP->SSP) | CAP REL97 |

テーブル II

【0042】

【表3】

トリプレット

| パラメータ | メッセージ | プロトコル |
|--|--|-----------------------------|
| RESULT Parameter: Authentication set パラメータ : 認証セット | SendAuthenticationInfo 認証情報の送信 (MSC/VLR -> HLR, VLRa -> VLRb) | MAP V1, V2, REL96, REL97 |

テーブル III

【0043】

上記例の結果は、すべてのメッセージにおいてこれらのパラメータが存在するわけではなく、通常は、機密性を要求する完全なメッセージのほんの一部にすぎ

ない。他の考慮では、アドレッシングの目的（例えば、シグナリング接続制御部（S C C P）など）で使用される情報が、M A PまたはC A Pプロトコル（例えば、国際移動電話加入者 I D（I M S I）、移動体サービス統合デジタル通信網（M S I S D N）、V L R数など）よりも下位のレベルでアクセスされてもよい。結果として、この情報についてのセキュリティーチェーンは無防備となり、応用部レベルでそれを保護するためには意味をなさない。

【0044】

従って、例示的な実施形態によれば、機密情報はパラメータレベルで暗号化されないので、クリアテキスト（C l e a r T e x t）部分からこれらのパラメータを削除し、これらはM A Pオペレーションの新しく暗号化（E n c r y p t e d）部分に含まれられ、例えば次のとおりである：

Param_1, Param_2, Param_3, Param_4

もしParam_2とParam_4が機密であるならば

ClearText (Param_1, Param_3), Encrypted (Param_2, Param_4)

【0045】

図6において示されたシーケンスは、暗号化されたパラメータの送信に対応する例示的なメッセージフローを示している。図6に示されるように、セキュリティ協定が受信エンティティとの間で確立されたかどうか、またはセキュリティ協定が満了したかどうかを、送信エンティティが検査する。もしセキュリティ協定がまだ確立されていないか、または、有効期間が満了しているならば、例えば、図5 Aにおいて示されているプロセスを使用して、セキュリティ協定が確立される。次に、情報とともにメッセージが送信される。（セキュリティ協定によって識別される）秘密パラメータは、送信エンティティにおいて暗号化される。そして、暗号化された情報を伴うメッセージが応答される。（セキュリティ協定によって識別される）秘密パラメータは、受信エンティティにおいて暗号化される。

【0046】

暗号化された情報は、新しい標準パラメータ（例えば、暗号化された情報など）に含まれられ、これらの内容は（タグと長さを除いて）完全に暗号化されている

。標準のセットと、ノーマルの符号化によって送信されるべきではないセンシティブな情報を含む所有パラメータとを暗号化された情報がふくんでもよい。この暗号化された情報のパラメータの内容は、メッセージを基礎として定義されてもよいし、または用可能なすべてのオペレーションにおいて使用可能な共通のデータタイプと定義されてもよく、オプションとして、センシティブな情報を備えることのできるすべてのパラメータが含まれよう。このパラメータは、認証情報、完全性情報、パディングオクテット及び選択されたセキュリティーメカニズムにより要求される他のすべての情報を含むことができる。

【0047】

暗号化された情報の選択は、確立されたセキュリティ協定に従って送信エンティティにおいて実行されてもよい。図7は、暗号化された情報を選択するための例示的なエンティティでのプロシージャ（手続）を示している。このプロセスはステップ700から開始される。ステップ710で、受信エンティティとのセキュリティ協定が確立されたかどうかが決定される。もし確立されていれば、ステップ720でセキュリティ協定の有効期間が満了したかどうかが決定される。もしステップ710で、受信エンティティとのセキュリティ協定が確立されていないと判定されたか、またはステップ720で、セキュリティ協定の有効期間が満了していると判定されたならば、ステップ730で、図5Aに示されるようなセキュリティ協定の確立手続が実行される。そして、ステップ740でセキュリティ協定が確立されるかどうかが決定される。もしステップ740でセキュリティ協定が確立されないと決定されれば、このプロセスはステップ780で終了する。

【0048】

ステップ790でセキュリティ協定の有効期間がまだ満了していないか、またはステップ740でセキュリティ協定がすでに確立されているとの決定から、この方法は、ステップ750に進み、そこでクリアテキストパラメータが準備される。ステップ760で、暗号化パラメータが準備される。ステップ770で、メッセージが送信され、ステップ780でプロセスが終了する。

【0049】

エンティティ認証

信頼されたエンティティに成りますことによって挿入されると、ネットワークにおいていくつかのオペレーションが要求していない行動を起こすかもしれない。原則として、すべてのオペレーションが違法な目的のために使用されるかもしれない。テーブル4においていくつかの例が与えられている：

【0050】

【表4】

| メッセージ | 効果 | プロトコル |
|---|---|-------|
| Update location 位置更新 (VLR->HLR) | Allow originating services to unregistered subscribers 発信サービスを未登録加入者に許可 | MAP |
| ProvideSubscriberInfo 加入者情報の提供 (HLR->MSC/VLR) | Allow unallowed terminating calls 無許可の着呼を許可 | MAP |
| InsertSubscriberData 加入者データ挿入 (HLR->VLR) | Allow services not provided to the subscriber 加入者へのサービスの非提供を許可 Allow arming CAMEL TAPS CAMEL TAPSの装備を許可 | MAP |
| InterrogateSS SS質問 (HLR->VLR) | Request subscriber information 加入者情報の要求 | MAP |
| Anytime interrogation 常時質問 (gsmSCF->HLR) | Request subscriber information 加入者情報の要求 | MAP |
| Initial DP DP開始 (gsmSSF->gsmSCF) | Its interception allows overcome possible controls 盗聴が可能な制御の克服を許可 | CAP |

テーブルIV

【0051】

上記の例から見てとれるように、異なるメッセージがネットワークの動作を異ならせるように影響するかもしれない。従って、結果として、すべてのエンティティが同一の認証要件を持っているわけではない。また、オペレーションに依存して、送信または受信エンティティが認証を要求してもよい（例えば、位置更新（LU）オペレーションにおいて、受信エンティティが認証を要求でき、一方で、挿入加入者データ（ISD）オペレーションにおいて、送信エンティティが認証を要求できる）。上述の暗号化に関しての他の考慮として、MAPやCAPプロトコルが認証を実現するための機能を備えている。

ロトコル（例えば、IMS1、MSISDN、VLR数、その他など）よりも下位のレベルにおいて、アドレッシングの目的（例えば、SCCPなど）で使用される情報がアクセスされ、変更されてもよい。結果として、応用部レベルで、この情報を保護するためには意味をなさない。

【0052】

例示的な実施形態によれば、エンティティ認証は、エンティティ基礎ごとに、選択されたオペレーションにだけ適用される。新しい認証（Authenticator）パラメータはMAPオペレーションの新しい暗号化された部分に含められてもよく、例えば：

Param_1, Param_2

もし送信エンティティが認証される必要があれば：

ClearText (Param_1, Param_2), Encrypted(Authenticator)

【0053】

エンティティ間で使用される認証には様々なタイプがある。

【0054】

例えば、タイプ1の認証において、機密性と信憑性とがキーのセキュリティーに基づくように、送信エンティティはドメインについてのキーを使用する。これは暗黙の認証を許可することになる。もしデジタル署名が新しいパラメータとしてメッセージに含められていれば、明示的な認証が可能となるであろう。

【0055】

タイプ2の認証においては、キー交換が開始されると、明示的な認証が可能となる。キーについての合意が確立されると、TTPから送信エンティティに証明書を提供できる。これにより、送信エンティティが証明書を受信エンティティに送信することが可能になる。キーがアクティブである期間は安全であると仮定すれば、送信エンティティだけが、そのセッションキーを使用して、暗号化された情報を受信エンティティに送信することができる。このケースの証明書は、 $K_{n2} [K_{sn1n2}, ID(N1), T, LK_{sn1n2}]$ であってもよい。キーがアクティブである期間にキーが安全であると仮定すれば、暗黙の認証が発生する。

【0056】

データが伝送されると、例えば、デジタル署名を使用して、明示的な認証が可能となる。例えば、ハッシュ機能を使用してメッセージによりメッセージダイジェストが生成され、それから、デジタルアルゴリズムをメッセージダイジェストに適用する。

【0057】

タイプ3の認証はタイプ2の認証と同様であり、このケースの証明書は $eKsn2 [eKpn2 [Ksn1n2, ID(N1), T, Lks] // TVP]$ であってもよい。明示的な署名もまた可能である。

【0058】

図8に示されたシーケンスは、認証情報を送信するためのメッセージフローを示す。第一に、送信エンティティは、セキュリティ協定が受信エンティティによって確立されたか、またはそれが満了したかを決定する。もしセキュリティ協定が確立されていないか、または、有効期間が満了していたならば、例えば、図5Aに示されたプロセスを使用してセキュリティ協定が確立される。次に、認証情報のメッセージが送信される。そして、（セキュリティ協定により識別される）認証パラメータは、送信エンティティにおいて暗号化される。認証情報を伴うメッセージが応答として送信される。（セキュリティ協定により識別される）認証パラメータは、受信エンティティにおいて暗号化される。

【0059】

認証情報は、上述の暗号化された情報パラメータの中への、新しい標準のパラメータ（例えば、entityAuthenticationInformation）に含まれられる。認証情報は通信エンティティの間で確立されたセキュリティ協定に従って、デジタル署名を含むコンテナに含まれられてもよい。

【0060】

図示されてはいないが、図7において示されたもの同様なエンティティ手続が、認証情報を送信するために実行されてもよい。

【0061】

データの完全性

例示的な実施形態によると、情報の完全性（Integrity）は、完全性情報を、メッセージ内容および他の潜在的な情報（例えば、TCP、タイム・スタンプ、シーケンス番号、その他など）に基づいて計算により求められたMAPオペレーションの暗号化された部分に含めることによって保証されてもよく、例えば：

Param_1, Param_2

もしメッセージの完全性が保証される必要があれば：

ClearText (Param_1, Param_2), Encrypted(Integrity)

【0062】

図9に示されたシーケンスは、完全性情報の送信に対応するメッセージフローを例示している。第一に、送信エンティティはセキュリティ協定が受信エンティティによって確立されたか、またはセキュリティ協定が満了したかを検査する。もし、セキュリティ協定が確立されていないか、または、有効期間が満了したならば、例えば、図5に示されたプロセスを使用して、セキュリティ協定が確立される。次に、完全性情報についてのメッセージが送信される。（セキュリティ協定により識別される）完全性のパラメータは、送信エンティティにおいて、メッセージ内容の関数として計算により求められ、番号化される。そして、完全性情報を伴うメッセージが応答として送信される。（セキュリティ協定により識別される）完全性パラメータは、受信エンティティにおいて暗号化される。

【0063】

完全性の情報は、上説のような暗号化された情報パラメータへの、新しい標準パラメータ（例えば、完全性情報）の中に含められる。

【0064】

図示は省略するが、図7において示されたものと同様なエンティティ手続が、完全性情報を送信するために実行されてもよい。

【0065】

例示的な実施形態によると、認証、暗号化、完全性、およびキー処理のためのメカニズムが、安全な通信を保証するために提供される。これにより、認証され

ないノードからのオペレーションが制限される。後方互換性が維持され、前方互換性が保証される。送信メカニズムは、キー処理および暗号化方法から独立している。暗号化／暗号解除に関連するオーバーヘッドが、セキュリティに敏感なメッセージ、パラメータ、および署名に追加されるだけである。

【0066】

GSMシステムのセキュリティーマネジメントに関連して、CCITT No.7のシグナリング、CAP及びMAPプロトコルを用いて説明してきたが、当業者であれば、本発明は、その必須の特徴を逸脱することなく、他の特定の形式でもって実施化が可能であることを明白に理解できよう。例えば、上述のセキュリティーマネジメントの原理は、他のタイプのシグナリングプロトコルおよび／または他のタイプの通信システムに適用されてもよい。従って、上で説明された実施形態は、限定のためではなく、説明に役立てるためのものであることがすべての点で考慮されるべきである。

【図面の簡単な説明】

発明の機能、目的、および利点は、同様な要素には同様の参照数字が付されている添付図面と連携しつつ説明を読むことによってより明白になろう。

【図1】

移動無線機通信システムのための例示的なネットワークアーキテクチャを示す図である。

【図2】

ローミング・シナリオについての例示的なネットワークアーキテクチャを示す図である。

【図3】

キーのライフサイクルを例示する図である。

【図4】

例示的な実施形態に従った安全な通信のためのシステムを示す図である。

【図5A】

キー管理情報を送信するためのメッセージシーケンスを示す図である。

【図5B】

セキュリティ協定を確立するためのプロセスの詳細な例を示す図である。

【図6】

暗号化された情報を送信するためのメッセージシーケンスを示す図である。

【図7】

暗号化された情報を送信するためのエンティティ手続を例示する図である。

【図8】

認証情報を送信するためのメッセージシーケンスを例示する図である。

【図9】

完全性に関する情報を送信するためのメッセージシーケンスを例示する図である。

【図1】

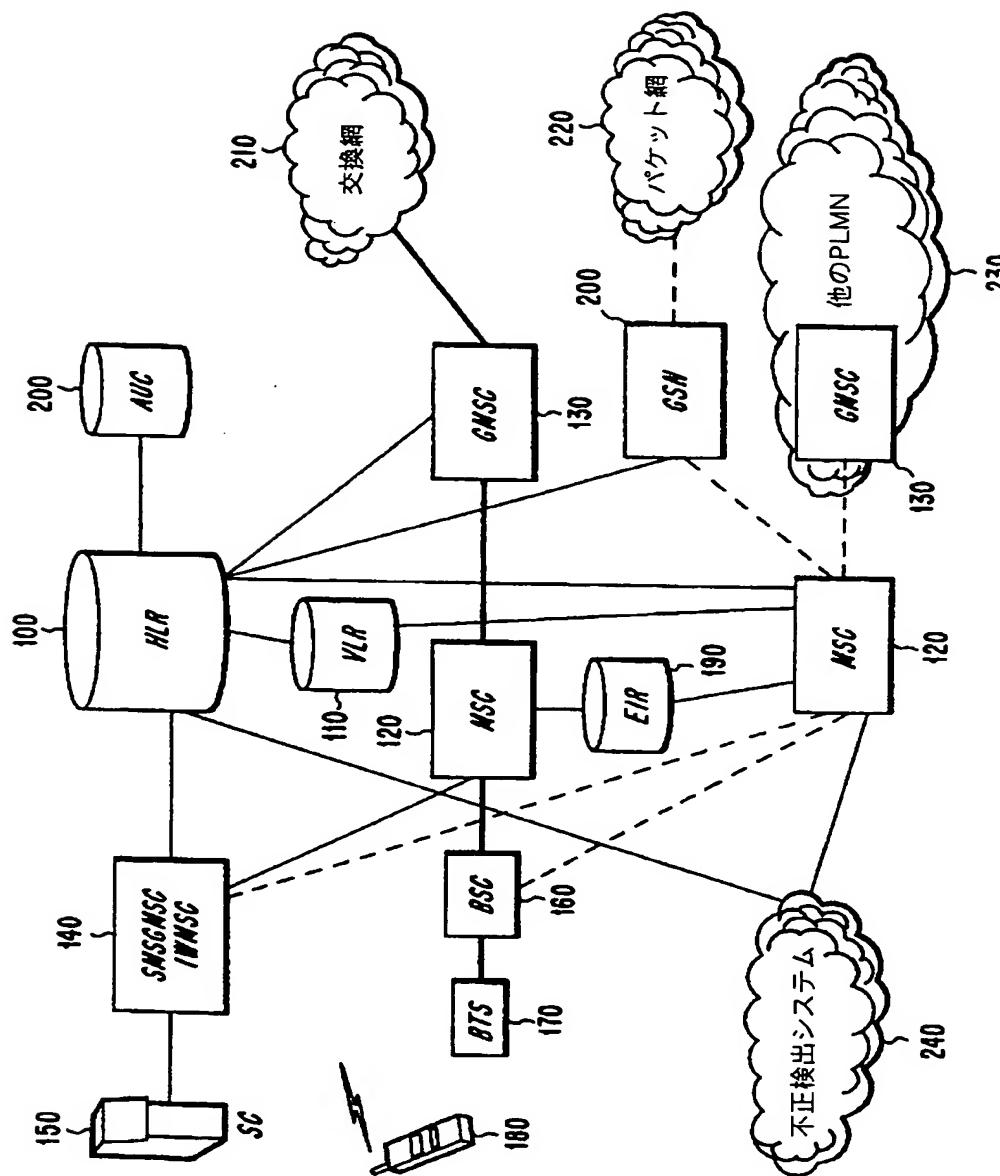
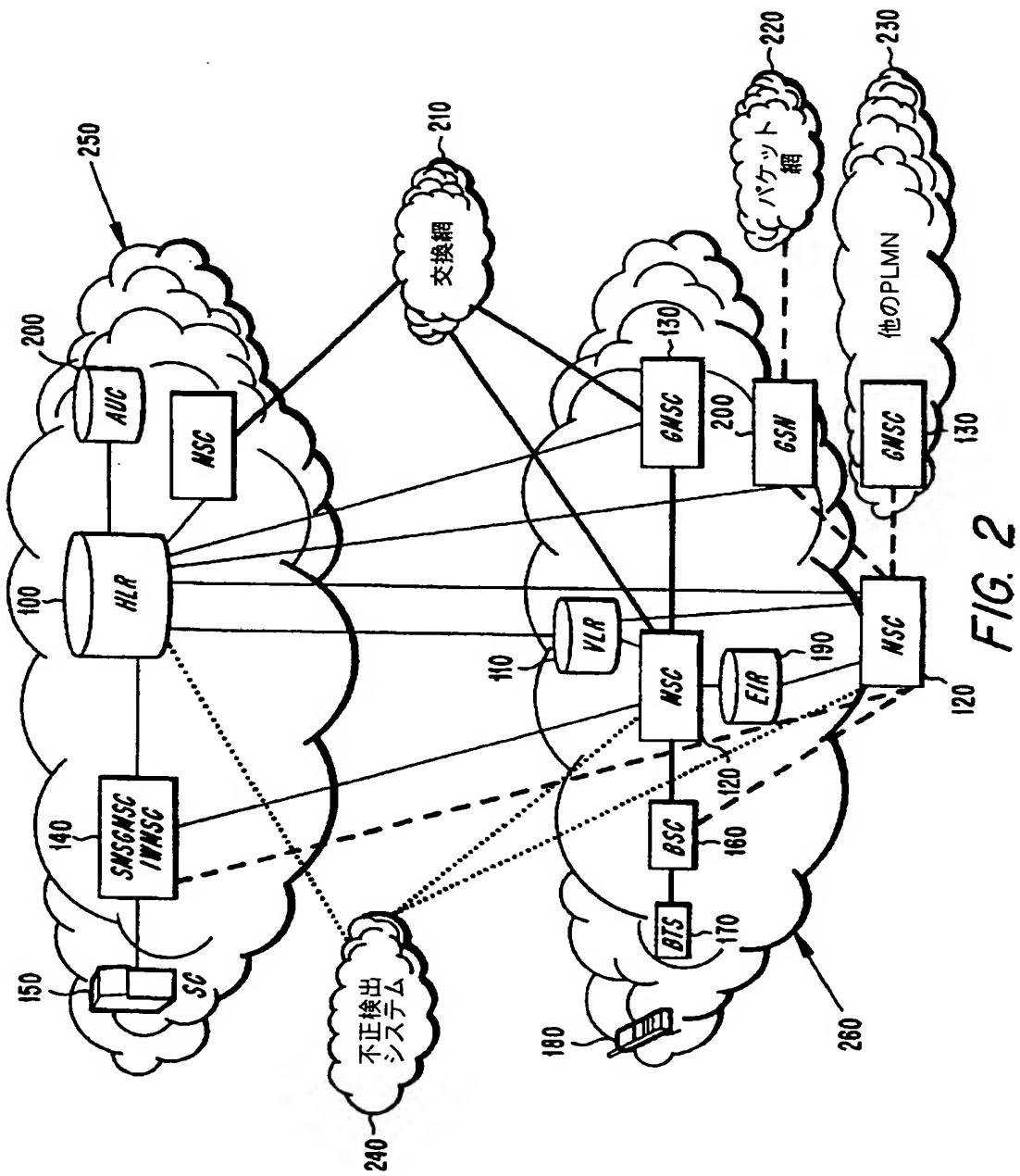


FIG. 1

【図2】



【図3】

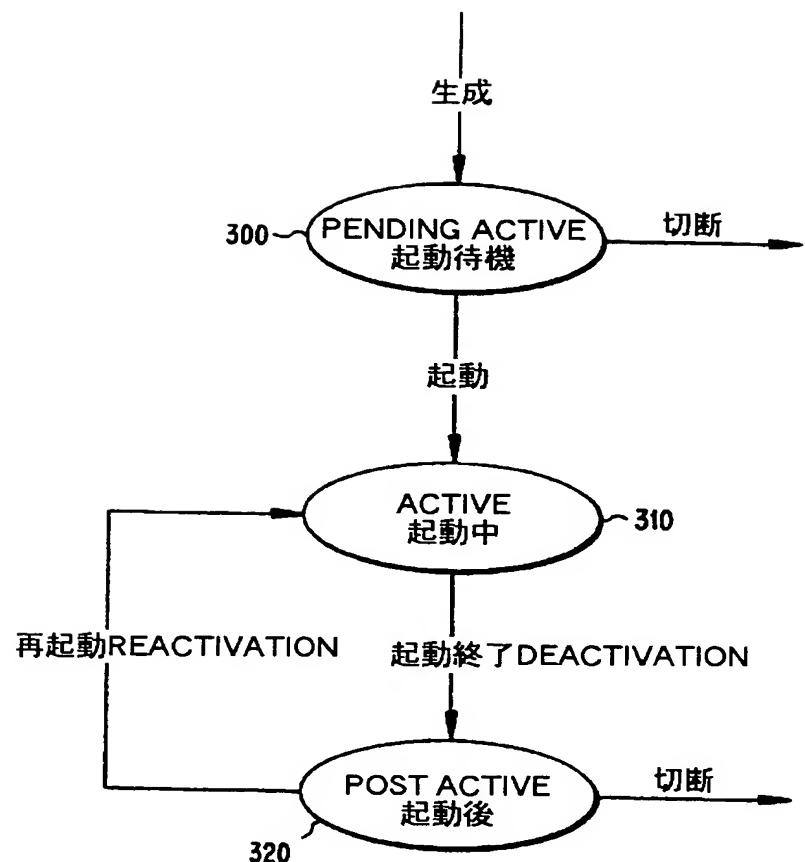
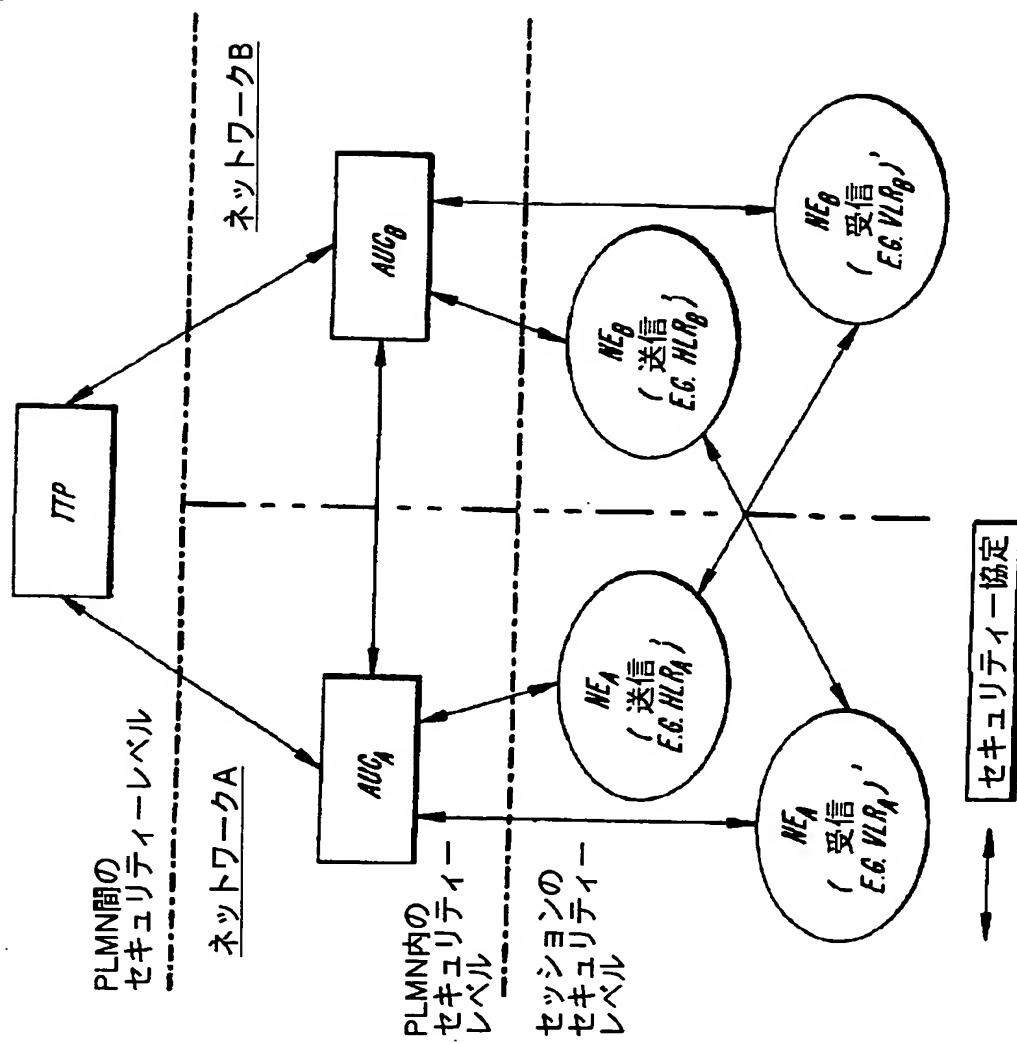


FIG. 3

【図4】

F/G. 4



【図5A】

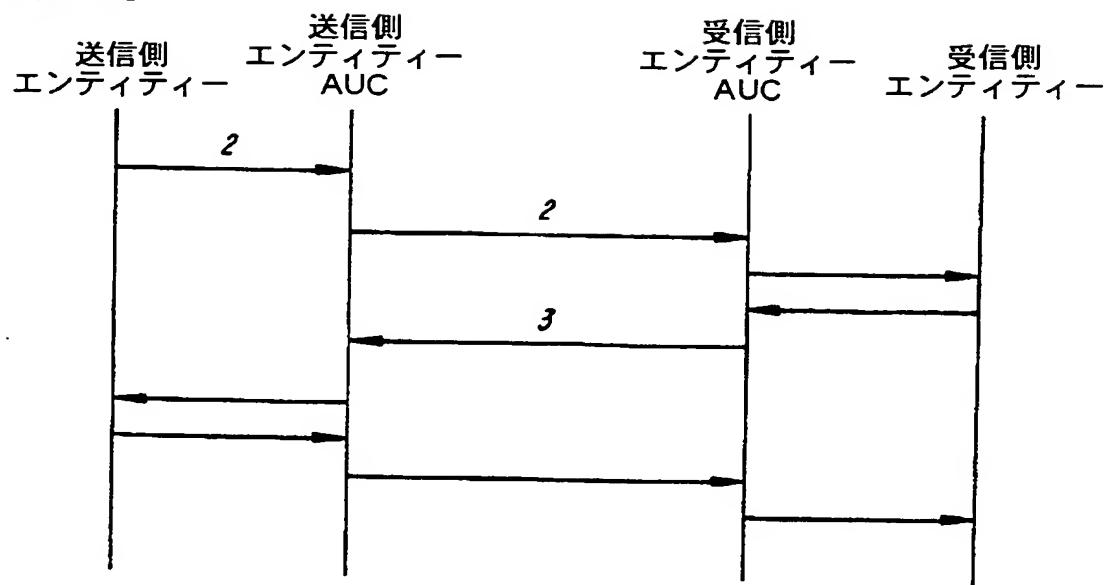
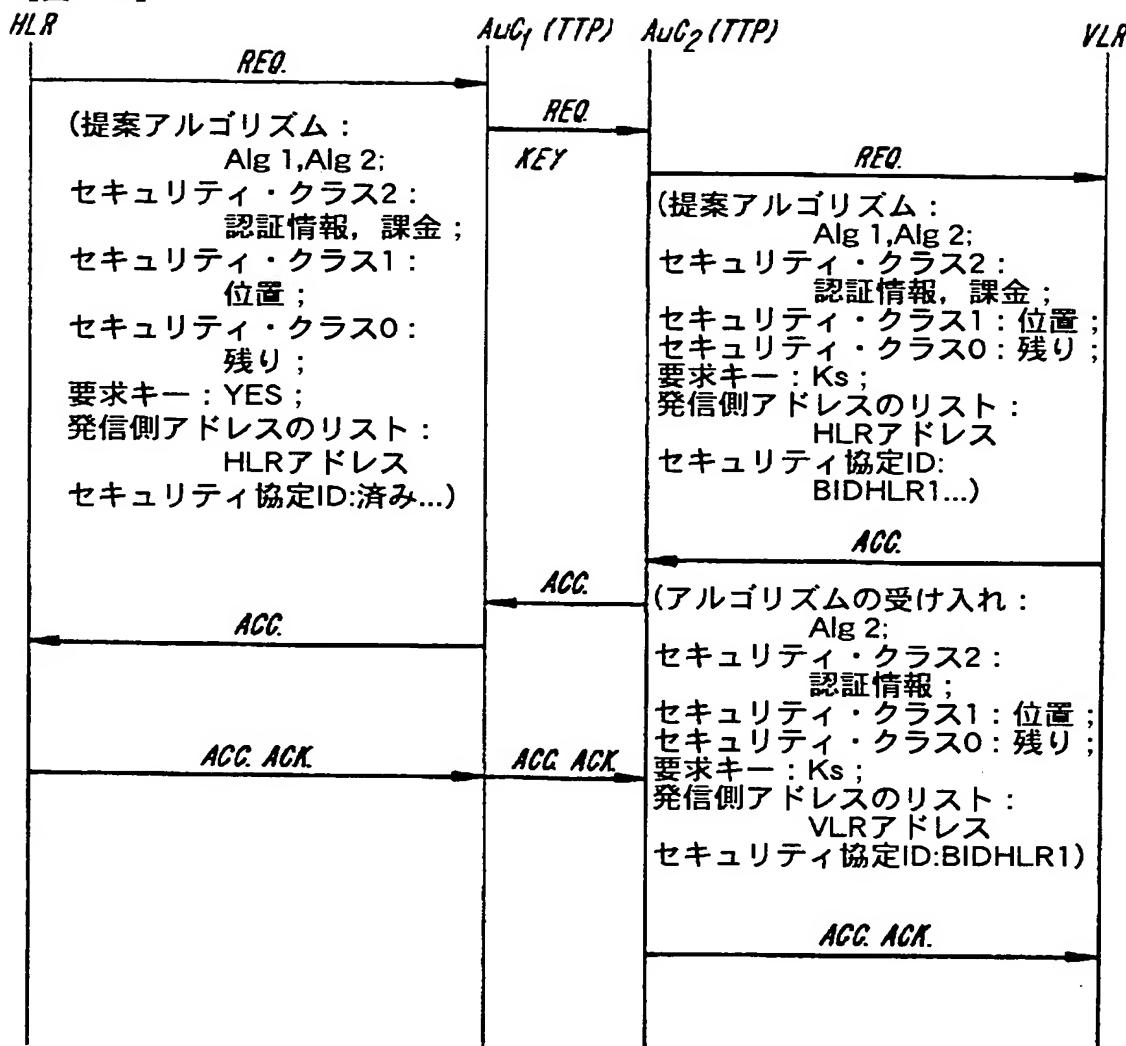


FIG. 5A

【図5B】

記憶される情報：

協定：BIDHLR1
アドレス：VLRアドレス
キー：Ks
パラメータ：認証情報：クラス2
：位置：クラス1
アルゴリズム：Alg2

記憶される情報：

協定：BIDHLR1
アドレス：HLRアドレス
キー：Ks
パラメータ：認証情報：クラス2
：位置：クラス1
アルゴリズム：Alg2

FIG. 5B

【図6】

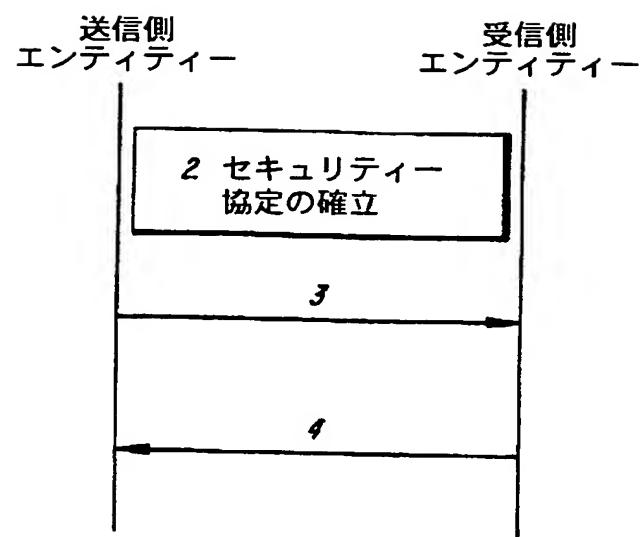
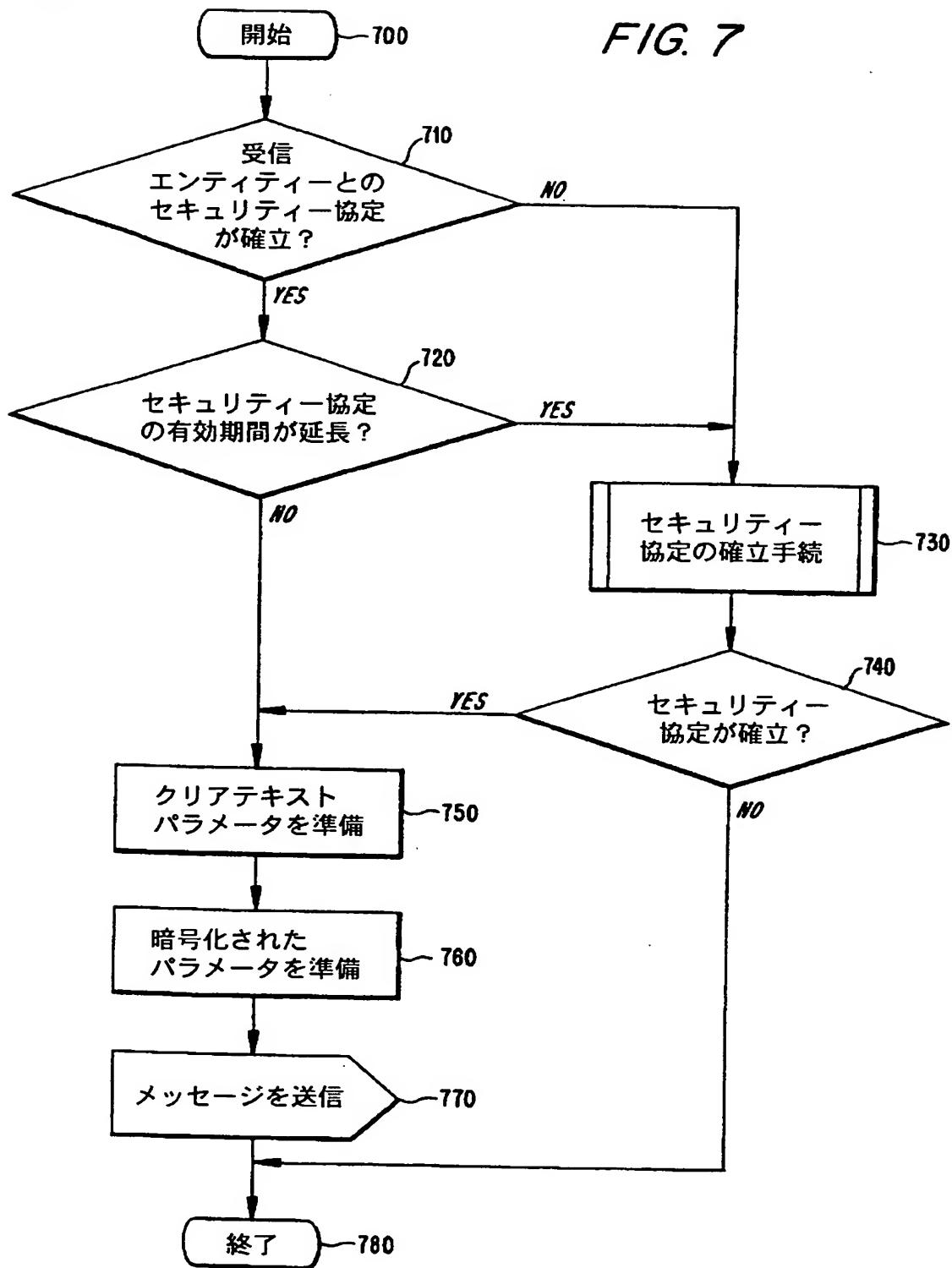


FIG. 6

【図7】



【図8】

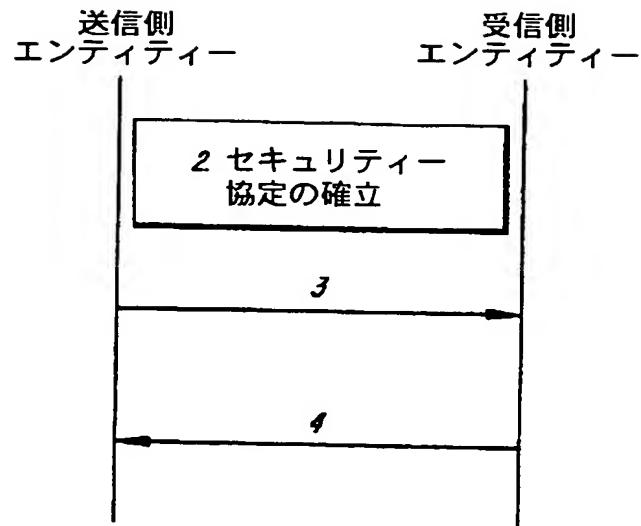


FIG. 8

【図9】

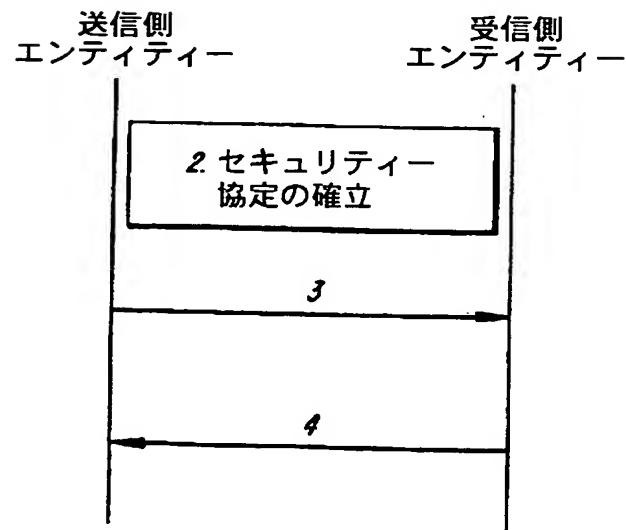


FIG. 9

【国際調査報告】

INTERNATIONAL SEARCH REPORT

| | | |
|---|--|--|
| A. CLASSIFICATION OF SUBJECT MATTER IPC 7 H04L29/06 | | Int'l. Appl. No. PCT/SE 00/01093 |
| According to International Patent Classification (IPC) or to both national classification and IPC | | |
| B. FIELDS SEARCHED Minimum documentation searched (classification systems followed by classification symbols) IPC 7 H04L H040 | | |
| Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched | | |
| Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal, WPI Data, PAJ, INSPEC | | |
| C. DOCUMENTS CONSIDERED TO BE RELEVANT | | |
| Category | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
| X | US 4 555 805 A (TALBOT ROBERT D) 26 November 1985 (1985-11-26) column 3, line 62 -column 4, line 31 --- | 1,2,4,5, 7-9,20, 21,23, 24,26-28 |
| X | US 4 920 567 A (MALEK CHARLES J) 24 April 1990 (1990-04-24) column 8, line 54 -column 9, line 48 --- | 1,2,4,5, 7-9,20, 21,23, 24,26-28 |
| A | GB 2 324 682 A (NIPPON ELECTRIC CO) 28 October 1998 (1998-10-28) page 3, line 14 -page 4, line 18 --- | 1-38 |
| <input type="checkbox"/> Further documents are listed in the continuation of box C. | | <input checked="" type="checkbox"/> Patent family members are listed in annex. |
| * Special categories of cited documents : | | |
| *A* document defining the general state of the art which is not considered to be of particular relevance | | |
| *E* earlier document but published on or after the international filing date | | |
| *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | | |
| *O* document referring to an oral disclosure, use, exhibition or other means | | |
| *P* document published prior to the international filing date but later than the priority date claimed | | |
| *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention | | |
| *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone | | |
| *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. | | |
| *Z* document member of the same patent family | | |
| Date of the actual completion of the international search | | Date of mailing of the international search report |
| 19 September 2000 | | 28/09/2000 |
| Name and mailing address of the ISA European Patent Office, P.O. 5818 Patentsteen 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tel. 31 651 epo NL Fax (+31-70) 340-3016 | | Authorized officer Weinmiller, J |

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/SE 00/01093

| Patent document cited in search report | Publication date | Patent family member(s) | | Publication date |
|--|------------------|-------------------------|------------|------------------|
| US 4555805 A | 26-11-1985 | US | 4411017 A | 18-10-1983 |
| US 4920567 A | 24-04-1990 | None | | |
| GB 2324682 A | 28-10-1998 | JP | 10215488 A | 11-08-1998 |
| | | AU | 5284598 A | 06-08-1998 |

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW

(72)発明者 カラトラバ レクエナ, オデリン
スペイン国 マドリッド エ-28027,
カージエ ヘネラル キルケバトリック,

6

Fターム(参考) 5J104 AA07 AA37 DA03 KA21 PA07
5K067 AA32 BB02 BB21 DD11 DD17
DD29 DD57 EE02 EE10 EE16
FF02 FF04 FF18 HH22 HH24
HH36

【要約の続き】

レスのリスト又はアドレスのグループおよび／またはセキュリティー協定の有効期間に関する情報などを含む。
暗号化、認証、および完全性はパラメータレベルで指定されてもよい。